Due Date: September 4, 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Raynold M. Kahn et al.	Examiner:	Pramila Parthasarathy
Serial No.:	10/758,811	Group Art Unit:	2136
Filed:	January 16, 2004	Docket:	PD-200290
Title:	DISTRIBUTION OF VIDEO CONTENT USING A TRUSTED NETWORK KEY FOR SHARING CONTENT		

CERTIFICATE OF MAILING OR TRANSMISSION UNDER 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office on September 4, 2008.

By:____________________
Name: Karen L. Lum

PETITION UNDER 37 C.F.R. §1.182

MAIL STOP PETITION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Petition is being submitted in accordance with M.P.E.P. §1002 to invoke the supervisory authority of the Director under 37 C.F.R. §1.182 involving the above-identified patent application.

REMARKS

On December 4, 2007, the Office issued a Non-Final Action in the above-entitled case. The Action:

- rejected claims 1-21 as unpatentable over amended claims 1-18 and 28-31 of copending application number 10/758,865; and
- rejected claims 1-21 as unpatentable over claims 1-39 of U.S. Patent no. 7,203,314

On March 4, 2008, the Applicants filed terminal disclaimers, for each of the above cases, mooting both rejections.

The Applicants hereby petition that these terminal disclaimers be withdrawn because they were unnecessary and improvidently filed. The rationale for the Applicant’s request is presented below.

I. CLAIMS 1-21 ARE NOT OBVIOUS OVER CLAIMS 1-39 OF U.S. PATENT NO. 7,203,314

The claims of the instant application are reproduced in Appendix I, and the claims of U.S. Patent No. 7,203,314 are reproduced in Appendix II.

As can be seen by inspection, none of these claims recites the use of a family key or anything analogous to it. Nor do the claims of the ‘314 patent recite the notion of a host receiver and a client receiver. Accordingly, the claims of the instant application are not obvious over the claims of 7,203,314.

The Office Action of December 4, 2007 argued:

> Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of instant claims “transmitting a family pairing key … generating a copy protection key … encrypting the decrypted program materials …. transferring the encrypted program material,” are referred to in the Patent claims as “… accepting encrypted access control information and the program material encrypted according to a first encryption key … a re-encryptor module, for re-encrypting the decrypted access control information … a copy protection module … to produce … encryption key”. Patent claims recite “a second decryptor module for decrypting the re-encrypted access control information to produce the first encryption key” which encompasses the instant application claims “generating the copy protection key at the client receiver using the family pairing key” and “decrypting the transferred program materials at the client receiver”. Thus the Patent claims anticipate the instant claims.

This is incorrect. The Office Action apparently analogized the instant application's "family pairing key" with the "encrypted access control information" of the issued patent. Even if the two were analogous (and they are not), the claims of the instant application recite the step of *generating a copy protection key at the host receiver using the family pairing key.* None of the claims of U.S. Patent No. 7,203,314 recite generating any key from the "encrypted access control information." Further, the claims of the instant patent recite the notion of host and client receiver and transferring program materials from the host receiver to the client receiver. This feature is entirely absent from the claims of the '314 patent. Finally, the claims of the instant application recite that the transferred program is decrypted using the copy protection key generated by the family pairing key. The '314 patent does not disclose decrypting materials using the copy protection key generated from a family pairing key or it's asserted analogue ... the "encrypted access control information."

Accordingly, the filing of the terminal disclaimer referring to the '314 patent was an error on the Applicant's part, and it is respectfully requested that this terminal disclaimer be withdrawn.

II. THE PROVISIONAL DOUBLE PATENTING REJECTION RELATING TO U.S. PATENT APPLICATION SERIAL NO. 10/758,865 WAS AND IS PREMATURE

MPEP § 804 (I)(B)(1) states:

> If a "provisional" nonstatutory obviousness-type double patenting (ODP) rejection is the only rejection remaining in the earlier filed of the two pending applications, while the later-filed application is rejectable on other grounds, the examiner should withdraw that rejection and permit the earlier-filed application to issue as a patent without a terminal disclaimer. If the ODP rejection is the only rejection remaining in the later-filed application, while the earlier-filed application is rejectable on other grounds, a terminal disclaimer must be required in the later-filed application before the rejection can be withdrawn.

In the instant case, assuming the terminal disclaimer and double patenting rejection relating to issued patent 7,203,314 (discussed above) is withdrawn, the nonstatutory obviousness-type double patenting rejection based on 10/758,865 is one of a number of provisional nonstatutory obviousness type double patenting rejections that are the only rejections remaining in this pending application. Further, application serial number 10/758,865 remains rejected on other grounds and issuance is not expected in the near future. Accordingly, the double patenting rejection of the instant case over the claims of 10/758,865 should be withdrawn.

III. CLAIMS 1-21 ARE NOT OBVIOUS OVER CLAIMS 1-39 OF U.S. PATENT APPLICATION SERIAL NO. 10/758,865

The claims of the instant application are reproduced in Appendix I, and the claims of U.S. Application Serial No. 10/758,865 are reproduced in Appendix III.

According to the Office Action,

> "all elements of instant claims correspond to the amended claims of the copending application, except in the instant claims "transmitting a family pairing key . . ., generating a copy protection key . . ., encrypting the decrypted program materials . . ., transferring the encrypted program material", are referred to in the amended copending application claims as "decrypting program materials . . ., encrypting the dcrypted program materials . . . transferring the encrypted program material". Copending claims recite "decrypting the transferred copy protection key at the client receiver . . . " and "decrypting the transferred program materials at the client receiver" which encompasses the instant application claims "generating the copy protection key at the client receiver using the family pairing key" and "decrypting the transferred program materials at the client receiver". Thus the copending application claims anticipates the instant claims."

The instant case recites the use of a family pairing key that is transmitted to the host and *used to generate a copy protection key that is then shared between the host and the client.* The claims of the '865 patent, however, recite a host-client pairing key that is generated by the service provider and shared between the host receiver and the client receiver. There is no notion of generating the copy protection key in the host from the pairing key. Therefore, even if the host-client pairing key were analogous to the family pairing key, it is generated differently and used differently. Accordingly, the instant application's claims are not obvious compared to the '865 patent claims.

IV. CONCLUSION

Accordingly, pursuant to MPEP § 1490 (VII)(A), the Applicants hereby petition the Director for relief in the form of withdrawing, nullifying, or otherwise canceling the terminal disclaimers mailed on March 4, 2008.

Applicant's request that should any fees be due for this Petition that they be charged to the Applicant's Deposit Account No. 50-0383. Please charge any additional fees or credit overpayment to Deposit Account No. 50-0383.

Respectfully submitted,

Date: September 4, 2008

Todd N Snyder

Todd N. Snyder, Registration No. 41,320
Attorney for Applicants

The DIRECTV Group, Inc.
CA / LA1 / A109
2230 E. Imperial Highway
El Segundo, CA 90245

Telephone No. (310) 964-0560

Appendix I

The Claims of the Instant Application

1. (ORIGINAL) A method of distributing video content from a broadcast system between a host receiver and a client receiver, comprising:

(a) transmitting a family pairing key from the broadcast system to both the host receiver and the client receiver;

(b) decrypting program materials received by the host receiver from the broadcast system;

(c) generating a copy protection key at the host receiver using the family pairing key;

(d) encrypting the decrypted program materials at the host receiver using the copy protection key;

(e) transferring the encrypted program materials from the host receiver to the client receiver;

(f) generating the copy protection key at the client receiver using the family pairing key; and

(g) decrypting the transferred program materials at the client receiver using the copy protection key.

2. (ORIGINAL) The method of claim 1, wherein the program materials received by the host receiver are encrypted using a media encryption key and the host receiver uses the media encryption key to decrypt the program materials.

3. (ORIGINAL) The method of claim 1, further comprising decrypting the family pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

4. (ORIGINAL) The method of claim 1, wherein the copy protection key is generated by the host receiver using content information decrypted by the family pairing key.

5. (ORIGINAL) The method of claim 4, wherein the content information comprises a content identifier.

6. (ORIGINAL) The method of claim 5, wherein the content identifier is obtained from the program materials.

7. (ORIGINAL) The method of claim 1, further comprising decrypting the family pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

8. (ORIGINAL) An apparatus for distributing video content from a broadcast system between a host receiver and a client receiver, comprising:

(a) means for transmitting a family pairing key from the broadcast system to both the host receiver and the client receiver;

(b) means for decrypting program materials received by the host receiver from the broadcast system;

(c) means for generating a copy protection key at the host receiver using the family pairing key;

(d) means for encrypting the decrypted program materials at the host receiver using the copy protection key;

(e) means for transferring the encrypted program materials from the host receiver to the client receiver;

(f) means for generating the copy protection key at the client receiver using the family pairing key; and

(g) means for decrypting the transferred program materials at the client receiver using the copy protection key.

9. (ORIGINAL) The apparatus of claim 8, wherein the program materials received by the host receiver are encrypted using a media encryption key and the host receiver uses the media encryption key to decrypt the program materials.

10. (ORIGINAL) The apparatus of claim 8, further comprising means for decrypting the family pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

11. (ORIGINAL) The apparatus of claim 8, wherein the copy protection key is generated by the host receiver using content information decrypted by the family pairing key.

12. (ORIGINAL) The apparatus of claim 11, wherein the content information comprises a content identifier.

13. (ORIGINAL) The apparatus of claim 12, wherein the content identifier is obtained from the program materials.

14. (ORIGINAL) The apparatus of claim 8, further comprising means for decrypting the family pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

15. (ORIGINAL) An article of manufacture embodying logic for performing a method of distributing video content from a broadcast system between a host receiver and a client receiver, comprising:

(a) transmitting a family pairing key from the broadcast system to both the host receiver and the client receiver;

(b) decrypting program materials received by the host receiver from the broadcast system;

(c) generating a copy protection key at the host receiver using the family pairing key;

(d) encrypting the decrypted program materials at the host receiver using the copy protection key;

(e) transferring the encrypted program materials from the host receiver to the client receiver;

(f) generating the copy protection key at the client receiver using the family pairing key; and

(g) decrypting the transferred program materials at the client receiver using the copy protection key.

16. (ORIGINAL) The article of claim 15, wherein the program materials received by the host receiver are encrypted using a media encryption key and the host receiver uses the media encryption key to decrypt the program materials.

17. (ORIGINAL) The article of claim 15, further comprising decrypting the family pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

18. (ORIGINAL) The article of claim 15, wherein the copy protection key is generated by the host receiver using content information decrypted by the family pairing key.

19. (ORIGINAL) The article of claim 18, wherein the content information comprises a content identifier.

20. (ORIGINAL) The article of claim 19, wherein the content identifier is obtained from the program materials.

21. (ORIGINAL) The article of claim 15, further comprising decrypting the family pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

Appendix II

The Claims of Issued Patent 7,203,314

1. A method of storing program material for subsequent replay, comprising the steps of:

receiving encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data;

decrypting the encrypted access control information to produce the temporally-variant control data;

modifying the temporally-variant control data to generate temporally-invariant control data;

re-encrypting the access control information including the temporally-invariant control data;

further encrypting the encrypted program material according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and storing the further encrypted program material and the encrypted access control information and the fourth encryption key.

2. The method of claim 1, wherein

the temporally-variant control data associates an expiration time with the program material and wherein: the step of modifying the temporally variant control data to generate temporally-invariant control data further comprises the steps of decrypting the received access control information to produce the first encryption key and the temporally-variant control data, and modifying the expiration time associated with the program material;

and the step of re-encrypting the access control information comprises the step of re-encrypting the first encryption key and the temporally-invariant control data.

3. The method of claim 1, wherein the step of re-encrypting the access control information comprises the step of encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fifth encryption key.

4. The method of claim 1, wherein: the step of modifying the temporally-variant control data to generate temporally invariant control data is performed by a smartcard.

5. The method of claim 1, further comprising the steps of:

retrieving the stored further encrypted program material, the encrypted access control information, and the encrypted fourth encryption key;

decrypting the encrypted fourth encryption key to produce the second encryption key using the third encryption key;

decrypting the further encrypted program material using the second encryption key;

decrypting the access control information to produce the first encryption key;

and decrypting the encrypted program material using the first encryption key.

6. The method of claim 5, wherein the step of decrypting the access control information to produce the first encryption key is performed in response to receiving a pay-per-view (PPV) request from the user.

7. The method of claim 5, further comprising the steps of:

further encrypting the encrypted access control information according to the second encryption key before storing the encrypted access control information;

and decrypting the further encrypted access control information according to the second encryption key to produce the encrypted temporally-invariant control data before decrypting the access control information.

8. The method of claim 7, wherein the step of decrypting the first encryption key is performed in response to receiving a pay-per-view request from the user.

9. The method of claim 1, wherein the steps of modifying the temporally-variant control data to generate temporally-invariant control data and re-encrypting the access control information including the temporally-invariant control data is performed in response to a pre-buy message.

10. The method of claim 1, wherein the access control information further comprises

metadata describing viewing rights for the program material.

11. The method of claim 10, further comprising the step of: generating the second encryption key from information including the metadata.

12. The method of claim 10, wherein the step of re-encrypting the access control information comprises the step of encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fourth encryption key, and the method further comprises the step of: generating the fourth encryption key from information including the metadata.

13. A method of storing program material for subsequent replay, comprising the steps of:

receiving access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and temporally-variant control data;

further encrypting the encrypted program material and temporally-variant control data according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and storing the further encrypted program material and the temporally-variant control data and the fourth encryption key.

14. The method of claim 13, wherein the temporally-variant control data associates broadcast channel and expiration time with the program material.

15. The method of claim 13, further comprising the steps of:

reading the stored further encrypted program material and the temporally-variant data and the fourth encryption key;

decrypting the fourth encryption key using the fourth encryption key to produce the second encryption key;

decrypting the further encrypted program material using the second encryption key;

decrypting the first encryption key using the fourth encryption key;

and decrypting the encrypted program material using the first encryption key.

16. An apparatus for storing program material for subsequent replay, comprising:

a conditional access module, for accepting encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including the first encryption key and temporally-variant control data, the conditional access module having a first decryptor module, for decrypting the encrypted access control information to produce the temporally variant control data;

a conversion module for modifying the temporally-variant control data to produce temporally-invariant control data;

a re-encryptor module, for re-encrypting the decrypted access control information;

a second decryptor module for decrypting the re-encrypted access control information to produce the first encryption key;

a copy protection encryption module, communicatively coupleable to the conditional access module and a media storage device, the copy protection encryption module for further encrypting the encrypted program material according to a second encryption key and for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and a copy protection decryption module, communicatively coupleable to the conditional access module and the media storage device, the copy protection decryption module for decrypting the encrypted fourth encryption key to produce the second encryption key using the third encryption key.

17. The apparatus of claim 16, further comprising: a tuner, communicatively coupleable to the conditional access module, for receiving the encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data.

18. The apparatus of claim 16, further comprising the media storage device.

19. The apparatus of claim 16, wherein:

the copy protection encryption module further encrypts re-encrypted access control information according to the second encryption key;

and the copy protection decryption module further decrypts the further encrypted re-encrypted access control information according to the second encryption key.

20. The apparatus of claim 16, wherein the temporally-variant control data associates an expiration time with the program material, and the conversion module modifies the expiration time associated with the program material.

21. The apparatus of claim 16, wherein the access control information further comprises metadata describing viewing rights for the program material and wherein the re-encryptor module re-encrypts the decrypted access control information according to a fifth encryption key generated at least in part from the metadata.

22. The apparatus of claim 16, wherein the access control information further comprises metadata describing viewing rights for the program material and the second encryption key is generated at least in part from the metadata.

23. The apparatus of claim 16, wherein the conditional access module is implemented in a smartcard.

24. The apparatus of claim 16, wherein the smartcard is releaseably communicatively coupleable with the tuner.

25. An apparatus for storing program material for subsequent replay, comprising:

means for receiving encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including a first encryption key and temporally-variant control data;

means for decrypting the encrypted access control information to produce the temporally-variant control data;

means for modifying the temporally-variant control data to generate temporally-invariant control data;

means for re-encrypting the access control information including the temporally-invariant control data;

means for further encrypting the encrypted program material according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and means for storing the further encrypted program material and the encrypted access control information and the fourth encryption key.

26. The apparatus of claim 25, wherein the temporally-variant control data associates an expiration time with the program material and wherein:

the means for modifying the temporally variant control data to generate temporally-invariant control data further comprises means for decrypting the received access control information to produce the first encryption key and the temporally-variant control data, and means for modifying the expiration time associated with the program material;

and the means for re-encrypting the access control information comprises the step of re-encrypting the first encryption key and the temporally-invariant control data.

27. The apparatus of claim 25, wherein the means for re-encrypting the access control information comprises means for encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fourth encryption key.

28. The apparatus of claim 25, wherein: the means for modifying the temporally-variant control data to generate temporally invariant control data is performed by a smartcard.

29. The apparatus of claim 25, further comprising:

means for retrieving the stored further encrypted program material, the encrypted access control information, and the encrypted fourth encryption key;

means for decrypting the encrypted fourth encryption key to produce the second encryption key using the third encryption key;

means for decrypting the further encrypted program material using the second encryption key;

means for decrypting the access control information to produce the first encryption key;

and means for decrypting the encrypted program material using the first encryption key.

30. The apparatus of claim 29, wherein the decryption of the access control information to produce the first encryption key is performed in response to receiving a pay-per-view (PPV) request from the user.

31. The apparatus of claim 29, further comprising:

means for further encrypting the encrypted access control information according to the second encryption key before storing the encrypted access control information;

and means for decrypting the further encrypted access control information according to the second encryption key to produce the encrypted temporally-invariant control data before decrypting the access control information.

32. The apparatus of claim 29, wherein the means for decrypting the first encryption key is performed in response to receiving a pay-per-view request from the user.

33. The apparatus of claim 25, wherein the means for modifying the temporally-variant control data to generate temporally-invariant control data and re-encrypting the access control information including the temporally-invariant control data is performed in response to a pre-buy message.

34. The apparatus of claim 25, wherein the access control information further comprises metadata describing viewing rights for the program material.

35. The apparatus of claim 34, further comprising: means for generating the second encryption key from information including the metadata.

36. The apparatus of claim 34, wherein the means for re-encrypting the access control information comprises means for encrypting the access control information including the temporally-invariant control data and the first encryption key according to a fourth encryption key, and the apparatus further comprises: means for generating the fourth encryption key from information including the metadata.

37. An apparatus for storing program material for subsequent replay, comprising:

means for receiving access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and temporally-variant control data;

means for further encrypting the encrypted program material and temporally-variant control data according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

and means for storing the further encrypted program material and the temporally-variant control data and the fourth encryption key.

38. The apparatus of claim 37, wherein the temporally-variant control data associates broadcast channel and expiration time with the program material.

39. The apparatus of claim 37, further comprising:

means for reading the stored further encrypted program material and the temporally-variant data and the fourth encryption key;

means for decrypting the fourth encryption key using the fourth encryption key to produce the second encryption key;

means for decrypting the further encrypted program material using the second encryption key;

means for decrypting the first encryption key using the fourth encryption key;

and means for decrypting the encrypted program material using the first encryption key.

Appendix III

Claims of U.S. Patent Application Serial No. 10/758,865

1. (PREVIOUSLY PRESENTED) A method of operatively pairing a host receiver and a client receiver in a broadcast system, comprising:

(a) receiving encrypted program materials, generated by a service provider, at one or more subscriber receiving stations, at least one of the subscriber receiving stations being comprised of a plurality of networked receivers, wherein the networked receivers include at least one host receiver and at least one client receiver;

(b) decrypting the received program materials at the host receiver;

(c) re-encrypting the decrypted program materials at the host receiver using a copy protection key;

(d) encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers;

(e) transferring the re-encrypted program materials and the encrypted copy protection key from the host receiver to the client receiver;

(f) decrypting the transferred copy protection key at the client receiver using the host-client pairing key; and

(g) decrypting the transferred program materials at the client receiver using the decrypted copy protection key.

2. (ORIGINAL) The method of claim 1, wherein the program materials received by the host receiver are decrypted using a media encryption key.

3. (ORIGINAL) The method of claim 1, wherein the host-client pairing key is received by both the host receiver and the client receiver from the broadcast system.

4. (ORIGINAL) The method of claim 3, further comprising decrypting the host-client pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

5. (ORIGINAL) The method of claim 4, wherein the copy protection key is generated by the host receiver using content information decrypted by the receiver key uniquely associated with the host receiver.

6. (ORIGINAL) The method of claim 5, wherein the content information comprises a content identifier.

7. (ORIGINAL) The method of claim 6, wherein the content identifier is obtained from the program materials.

8. (ORIGINAL) The method of claim 6, wherein the content identifier further comprises copy control information.

9. (ORIGINAL) The method of claim 3, further comprising decrypting the host-client pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

10. (PREVIOUSLY PRESENTED) An apparatus for operatively pairing a host receiver and a client receiver in a broadcast system, comprising:

(a) means for receiving encrypted program materials, generated by a service provider, at one or more subscriber receiving stations, at least one of the subscriber receiving stations being comprised of a plurality of networked receivers, wherein the networked receivers include at least one host receiver and at least one client receiver;

(b) means for decrypting the received program materials at the host receiver;

(c) means for re-encrypting the decrypted program materials at the host receiver using a copy protection key;

(d) means for encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers;

(e) means for transferring the re-encrypted program materials and the encrypted copy protection key from the host receiver to the client receiver;

(f) means for decrypting the transferred copy protection key at the client receiver using the host-client pairing key; and

(g) means for decrypting the transferred program materials at the client receiver using the decrypted copy protection key.

11. (ORIGINAL) The apparatus of claim 10, wherein the program materials received by the host receiver are decrypted using a media encryption key.

12. (ORIGINAL) The apparatus of claim 10, wherein the host-client pairing key is received by both the host receiver and the client receiver from the broadcast system.

13. (ORIGINAL) The apparatus of claim 12, further comprising means for decrypting the host-client pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

14. (ORIGINAL) The apparatus of claim 13, wherein the copy protection key is generated by the host receiver using content information decrypted by the receiver key uniquely associated with the host receiver.

15. (ORIGINAL) The apparatus of claim 14, wherein the content information comprises a content identifier.

16. (PREVIOUSLY PRESENTED) The apparatus of claim 15, wherein the content identifier is obtained from the program materials.

17. (ORIGINAL) The apparatus of claim 16, wherein the content identifier further comprises copy control information.

18. (ORIGINAL) The apparatus of claim 12, further comprising means for decrypting the host-client pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

19-27. (CANCELED)

28. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the particular combination of the host and client receivers results in a different host-client pairing key for each pairing of the client receiver with the host receiver.

29. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the particular combination of the host and client receivers results in the host receiver sharing the host-client pairing key with all client receivers.

30. (PREVIOUSLY PRESENTED) The apparatus of claim 10, wherein the particular combination of the host and client receivers results in a different host-client pairing key for each pairing of the client receiver with the host receiver.

31. (PREVIOUSLY PRESENTED) The apparatus of claim 10, wherein the particular combination of the host and client receivers results in the host receiver sharing the host-client pairing key with all client receivers.